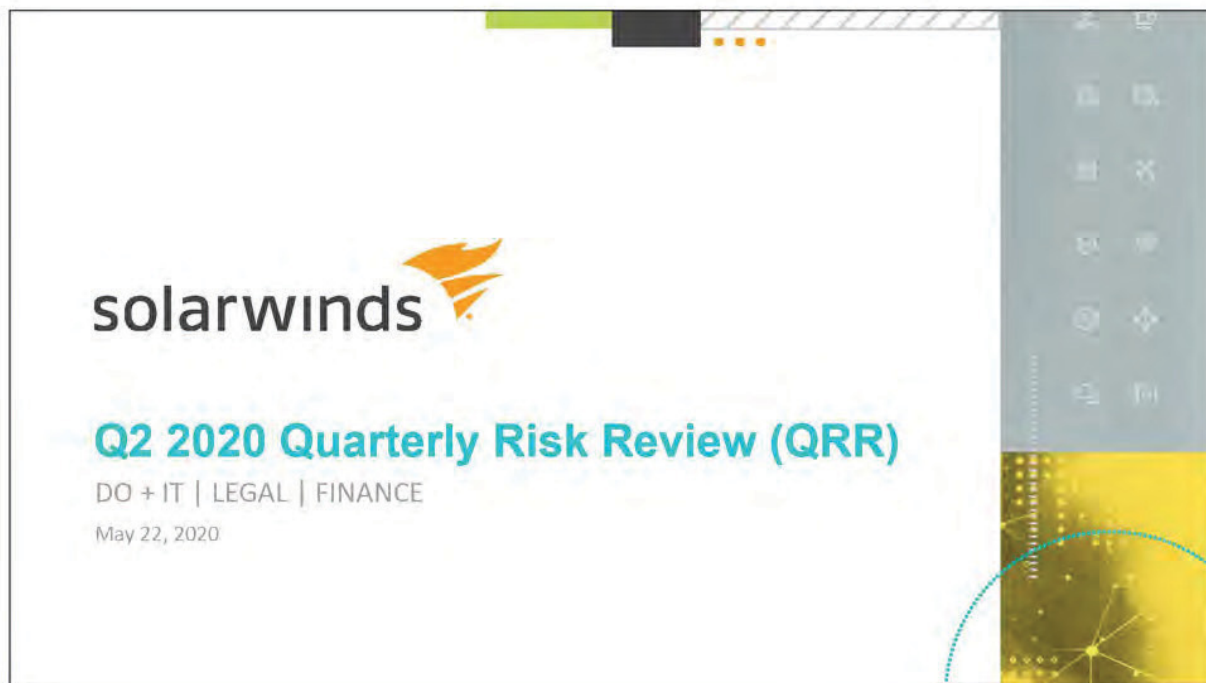


EXHIBIT C

Excerpts of SW-SEC000148267



5/21/20: i

@solarwinds

Q1 2020 AD Access Audit Deficiency | Remediation

PRELIMINARY ROOT CAUSE ANALYSIS (RCA) Active Directory Access Review Audit Deficiency (SOX ITGC)

Materiality: Q1 2020 Affected Service: SOX ITGC Severity: High - Control Deficiency

Incident Summary

The Q1 2020 Services Only (SOX) Information Technology General Controls (ITGC) stipulate that user privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory) and databases.

During the Q1 2020 internal audit of Active Directory on 5/4/2021, PwC auditors and Internal Audit determined the AD Q1 audit did not sufficiently review the objective, as it was unclear if AD users were active and that their access was appropriate.

During the RCA investigation, two major breakdowns are attributed to 1) inconsistent data for contractors and vendors, and the need for a single source of truth and 2) the overall AD Audit review process did not fully meet the audit objectives. These breakdowns created risk of unauthorized users having inappropriate access to AD.

As a result of the RCA, the following corrective actions have been immediately implemented:

- Vendors and Contractors have been consolidated into a single, centrally managed list and a process has been established for hiring managers to request, change and/or remove AD access.
- The Service Desk team has reviewed 343 individuals identified during the first audit as requiring validation and re-run the audit with May information to affirm appropriate access has been established.
- The Service Desk team identified 18 additional individuals who were identified as active, however were inactive contractors and/or vendors.

In addition to these immediate steps, there are plans to automate the audit process, and incorporate vendors and contractors into the HRIS system (est. 2021).

Root Cause

The ITGC Q1 2020 User Access Review for AD failed due to incomplete data and an incomplete audit process, as outlined below:

No.	Issue	AD User Access Management (ITGC)	Root Cause	Impact
1	Inconsistent Vendor and Contractor Data	The Vendor and Contractor lists used to validate the AD User data was incomplete.	No single authoritative source of truth.	Audit failure due to incomplete data reported in the appearance of 325 users, potentially having inappropriate access to AD.
2	Audit Process did not meet audit objective	The AD UAR was unable to demonstrate if AD users were active and if their access was appropriate.	Process design did not meet audit objectives.	Audit failure due to process design not adequately demonstrating objective.

	Authorized	Unauthorized	Grand Total
Employee in Updated List	198	9	207
SolarPeople	132		132
Vendor List - Flexis	18		18
SolarPeople - Intern	11	2	13
Contractor List - Mina	12		12
Vendor	11	1	12
Vendor List - Michal	8		8
Contractor	6	1	7
No Show Day 1 - No SARF Term Received		3	3
No SARF Term Received	1	1	1
SARF Term Sent Late		1	1
Timing Issue	14		14
SARF Term	7		7
New Hire	7		7
Not on Managed List	83	21	104
Vendor	53	1	54
Contractor	18	9	27
MSA	12	2	14
Unknown		6	6
Employee		3	3
Erroneously excluded from audit		18	21
Grand Total	295	48	343

Key Corrective Actions

- Created authoritative list of vendors and contractors
- Redefined audit procedures

@solarwinds